Features Editor: Tyrus L. Manuel ✉ tmanuel@computer.org

After ElcomSoft: DMCA Still Worries Developers, Researchers

Laurianne McLaughlin

There should have been a collective sigh of relief in December 2002, when a US federal jury acquitted Russian software firm ElcomSoft of criminal charges stemming from the Digital Millennium Copyright Act. The jury decided that ElcomSoft did not knowingly violate the DMCA law when it created a new type of reader software for Adobe eBook files. ElcomSoft liked the acquittal, no matter the legal reasoning. But there was little rejoicing among software developers, security researchers, consumer advocates, and legislators who've been fighting the DMCA. As a test of the law itself, this trial didn't deliver a knockout punch.

Ever since the US Congress passed the hotly debated DMCA law in 1998, intending to address copyright issues in the Internet age and satisfy some aspects of the 1996 World Intellectual Property Organization Treaty, developers and researchers have watched and waited to see how the law would apply to companies working at the edge of existing technologies.

The ElcomSoft acquittal has lessons containing good and bad news for the software and research communities. The trial eliminated some of the fear of the unknown surrounding prosecutions. But more notably, the threat of legal action still looms, and the specific language of the DMCA law troubling the scientific community still stands. Also, legal experts say that ElcomSoft's "I didn't know better" defense probably won't work in future cases. DMCA opponents must continue their battle against the law.

Another unexpected outcome of ElcomSoft's struggle is clear: The ElcomSoft trial and a January 2003 US Supreme Court decision, *Eldred et al. vs. Ashcroft*, have stirred up public interest in the DMCA and copyright law. (The Eldred case upheld the Sonny Bono Copyright Term Extension Act and added 20 years to copyright life.) Consumers are asking whether the DMCA too narrowly restricts their rights to use media such as music and books, and whether it stifles technology progress in areas such as online security, a key concern in a time of heightened political tension.

This development, along with a recently reintroduced Congressional bill to amend the DMCA, provides some encouragement to software and security experts who disagree with the law's scope.

ElcomSoft's problem

ElcomSoft's struggle began in the summer of 2001, when FBI agents took ElcomSoft programmer Dmitry Sklyarov into custody during the Defcon convention in Las Vegas.

ElcomSoft had developed a reader program for Adobe eBook files that let users turn eBook files into Adobe Portable Document Format (PDF) files. Adobe Systems maintained that developing such a reader violated the DMCA's "anticircumvention" provisions, spelled out in section 1201 of the law. These provisions—which are at the heart of the software and security community's problems with the DMCA—aim to stop counterfeiters or hackers from unraveling technological protections on copy-

0740-7459/03/$17.00 © 2003 IEEE

righted material, such as DVD movies.

Section 1201 prohibits the act of developing technology that "circumvents technological measures" designed to protect copyrighted material. It also prohibits selling or distributing the tools used to circumvent the technological measures. Civil and criminal charges can apply to violations. Section 1201 includes some exceptions—for example, for encryption research. But a literal reading of the section's wording has created "unwarranted prosecutions," says US Representative Rick Boucher (Democrat, Virginia), who's leading a legislative charge to amend the DMCA.

Note that ElcomSoft wasn't charged with trying to pirate eBooks, nor was Sklyarov. The ElcomSoft reader could be used for such purposes as backing up an eBook file or reading an eBook file on a Linux PC instead of a Windows or Mac system. However, Adobe argued that creating and distributing the technology—circumventing the protection mechanisms in the eBook files—broke the DMCA rules. Theoretically, a company with other intentions could use the reader later, to facilitate copying copyrighted eBooks.

Ultimately, the court dropped personal charges against Sklyarov. During the December 2002 trial against ElcomSoft, the judge told jurors that to convict ElcomSoft, they had to decide that the company willfully violated the legal rules. The company launched a successful defense that hinged on this point.

The legal fallout

This defense strategy bears close examination by the software community. On one hand, it sends prosecutors a message that cases will have to be more clear-cut than ElcomSoft's to earn a conviction.

"I expect that future criminal prosecutions under the DMCA will be limited to real piracy cases," says Orin Kerr, an associate professor at George Washington University Law School, whose specialties include Internet law. "Close cases will not be indicted."

Still, scientists and software developers can't take too much comfort in the ElcomSoft outcome, says Atlanta attorney Doug Isenberg, who practices Internet and intellectual-property law and runs the GigaLaw.com Web site. "The DMCA is still alive and well and on the books," he says. "This case was about one defendant and how to interpret the DMCA. It didn't say the law was unconstitutional or unenforceable. Just because ElcomSoft was found not guilty, it doesn't mean that others who engage in similar activities aren't in violation of the DMCA."

So, ElcomSoft's case did not reduce the security community's concerns surrounding the DMCA, states security expert Bruce Schneier, founder and chief technology officer at Counterpane Internet Security. Researchers have no more latitude today than they did before ElcomSoft, he says.

"The DMCA is not about prosecution, it's about the threat of prosecution," Schneier explains. "Companies are using the DMCA to threaten individuals and companies into submission. It is my hope that the ElcomSoft decision will embolden people to stand up to the threats, but it probably won't. Threats are more about who has the deeper pockets than anything else."

The DMCA as competitive tool

Businesses increasingly use DMCA lawsuits as a competitive tool, to slow down or hurt their rivals, Schneier and other DMCA critics point out. In an ongoing case, printer maker Lexmark has filed suit against Static Control Components, a North Carolina company that makes and sells control chips to third-party manufacturers of printer toner cartridges.

Businesses increasingly use DMCA lawsuits as a competitive tool, to slow down or hurt their rivals.

Lexmark, not surprisingly, wants exclusive control over replacement supplies for its printers. Lexmark replacement cartridges have a microchip that takes part in what Lexmark calls "authentication sequence" technology. An electronic handshake, done when you replace a cartridge, tells a Lexmark printer that it's talking to a Lexmark cartridge.

Static's chips allow third-party cartridges to speak to the Lexmark printers and give a handshake that works. Lexmark claims that when a Static chip mimics the authentication sequence, it violates the DMCA's anticircumvention provisions.

Static agreed in early January to stop selling the chips until the US District Court in Lexington, Kentucky, hears the case.

In another recent example, Chamberlain Group, a garage-door-opener manufacturer, has launched a DMCA lawsuit against Skylink Technologies. Chamberlain argues that Skylink's technology, which lets third-party remote controls work with Chamberlain door openers, violates the DMCA anticircumvention provisions.

Groups such as the Electronic Frontier Foundation state that these types of interpretations of the provisions go too far. The clause's language has been written too broadly, they argue, inhibiting competition and innovation.

Software and research questions

The parallels to the Lexmark case seem keen for software developers and Internet security researchers whose work involves reverse engineering to improve a technology, test its strength, or construct an alternative.

"Reverse engineering is vital to security," Schneier states. "As long as companies lie about the security of their software and systems, the only

way to find out the truth is to reverse-engineer the software."

In one of the first high-profile DMCA cases, Princeton University's Edward Felten was threatened with a DMCA suit as he and a group of researchers prepared to present a paper on watermarking technologies related to digital music.

Felten's case pointed out a key problem with the DMCA's anticircumvention provisions, critics say. Their argument: To strengthen technologies, including those protecting digital media, researchers often must take those technologies apart. If they can't do so without violating the provisions, the research might not get done. Security innovations could stall, and what's more, the market for the digital media itself could weaken.

"The (DMCA) law was passed at a time when technology and applications of that technology were evolving quickly," says George Cybenko, Dartmouth College professor of engineering (and editor in chief of *IEEE Security & Privacy*). "The implications for security research weren't well understood or anticipated."

Cybenko recommends that if a university research team is doing work that could create DMCA legal problems, it should strike up-front agreements with the owners of the related intellectual property.

Felten's case and the other challenges using section 1201 give academics and researchers reason to think harder about the parameters of the DMCA rules, Cybenko says. ElcomSoft's acquittal leaves situations like Felten's still liable to occur.

Boucher Bill proposes remedy

In fact, Felten's case is one factor that led Representative Boucher to introduce legislation to amend the DMCA. The Digital Media Consumers' Rights Act, also known as the Boucher Bill (H.R. 107), broadens the exceptions to the DMCA's anticircumvention rules.

It lets researchers carry out "scientific research into technological protection measures" and develop the necessary software tools for that research. While the current law has an exception for some types of encryption research, Boucher's bill widens the types of research allowed.

"For example, if you're testing the strength of a digital watermark, potentially you wouldn't be able to do that under the current exemption," Boucher explains. "It's in the interest of everyone to know the quality of the technology."

Also, if a company's technology equipment is capable of a "substantial noninfringing use," the manufacturer would not be liable under the DMCA. ElcomSoft's case is a good example of where this amendment would change the rules, Boucher says. A consumer porting the text of an eBook for backup purposes, for example, is not a copyright-infringing use. "Because it was subject to 'possible' misuse, ElcomSoft was prosecuted," he says.

His bill also protects the rights of consumers to make backup copies and requires clear labeling on copy-protected CDs that won't play in certain DVD or CD players.

The measure sits before the House Commerce Committee, and Boucher expects a hearing within a few months. He's fighting determined, well-financed opponents in the movie and recording industries.

Still, he's optimistic. "I've got some deep pockets on my side too," he says, citing support for his bill from technology companies including Intel, Sun Microsystems, and Gateway. "I've also got a very strong public-interest community," he adds, noting backing from the American Library Association, the Association of American Universities, and the Consumers Union.

The ElcomSoft case has helped the bill's chances, Boucher believes. "The prosecution of ElcomSoft created a tremendous backlash among the American public to the provisions of the DMCA and alerted Americans to the harm the DMCA causes to innovation," Boucher explains. "We now have many people mobilized who will fight."

While ElcomSoft's case raised awareness regarding the DMCA inside the United States, it left many questions unanswered for companies elsewhere.

Offshore confusion

While ElcomSoft's case raised awareness regarding the DMCA inside the United States, it left many questions unanswered for companies elsewhere. Some people had hoped the case would have more clear-cut lessons. This case did not give non-US software companies any improved legal footing regarding the DMCA, legal experts claim.

"The lesson generally of the digital copyright cases is that the arm of US law is very long indeed," says Mark Lemley, professor at the University of California at Berkeley's Boalt Hall School of Law, and counsel to Keker & Van Nest LLP, where he specializes in antitrust, intellectual property, and computer law. (The firm represented programmer Dmitry Sklyarov in the ElcomSoft case.)

File-sharing service Kazaa remains locked in what's perhaps the most closely watched copyright dispute involving cross-border issues. Sharman Networks, the company that runs Kazaa, is fighting a fierce court battle regarding jurisdiction. The company, based in Australia, faces a suit from the Recording Industry of America and the Motion Picture Association of America regarding copyright infringement of music files, among other things.

In early January, a federal judge in Los Angeles declared the two groups could sue Sharman Networks in the

US, noting the millions of US users of the service and the California addresses of music and motion picture heavyweights. In late January, Sharman filed a countersuit that includes antitrust allegations. The case will likely continue for some time. In the meanwhile, ElcomSoft's recent experience doesn't give Sharman much useful legal ammunition.

Even putting aside the long-simmering music copyright issues and focusing more on technology research, non-US companies remain confused about what kind of action violates the DMCA, states Isenberg, adding that the arrest of ElcomSoft's programmer sent one message clearly. "If I am a businessperson in another country and I have any potential concerns that my products would violate the DMCA, I'd be hesitant to make a public presentation in the United States," he says.

Would the threat of DMCA prosecution actually send US software or security companies offshore? That's pretty unlikely, given the state of the law, Isenberg predicts. While some Internet enterprises, such as gambling sites, have purposefully set up outside the United States, there's no evidence that technology companies are leaving for this reason.

What's next

For now, companies and researchers can immediately take one piece of advice resulting from the ElcomSoft case under advisement. ElcomSoft's defense won't work for much longer, Isenberg states. "As the DMCA becomes well known, it will be harder to plead ignorance," he adds.

If you're looking for ways to keep up with developments relating to the DMCA, check out Felten's weblog at www.freedomtotinker.com and Lawrence Lessig's weblog at http://cyberlaw.stanford.edu/lessig/blog. (Lessig represented the lead plaintiff in the *Eldred* Supreme Court case.)

It's a little too early to tell whether the Boucher Bill will succeed or, alternatively, whether a court case could solve the problems of the DMCA for the software and security communities. The opinions of Internet law watchers vary on whether the chances for modifying the DMCA look better in the legislature or the courts.

"As the US Supreme Court's recent Eldred decision shows, the courts don't like to step in to these disputes, even when Congress passes a bad statute," Kerr says. "These battles have to be won in Congress, not the courts."

However, the DMCA's real legal test might be yet to come, for two reasons, explains Mark Lemley. "First, the ElcomSoft court held that the DMCA was constitutional, but because ElcomSoft was acquitted, the case is over and ElcomSoft can't appeal that ruling," he says. "So the issue of constitutionality never got finally resolved."

Second, in ElcomSoft's case and the Corley case of 2001 (in which a Web site was prohibited from posting DeCSS code related to DVD encoding), the courts based their reasoning on their belief that fair use was not constitutionally required, Lemley says. "The Supreme Court held ... in Eldred that fair use is constitutionally required. That will force courts to rethink the constitutionality of the DMCA," he predicts.

The software community also has history on its side, Lemley adds. "Copyright and trade secret owners fought for years to ban reverse engineering in the software industries, arguing that reverse engineering violated copyright law," he explains. "The courts rejected this argument and held reverse engineering legal. The software industry did not collapse as a result; in fact, it flourished."

Software Language Should Help Protect Networks from Hackers

Terry Costlow

Preventing hackers and criminals from slipping into computer networks is a growing challenge, one that appears destined to get more difficult every year. However, new tools and standards are emerging, giving those entrusted with protecting networks new ways to spot the vulnerabilities and exposures where intruders enter.

Last year, MITRE unveiled a standard that gives tool developers a common way to check for and identify these vulnerabilities and exposures. The Open Vulnerability Assessment Language (http://oval.mitre.org) provides a consistent language so that security experts can discuss the minute details of the techniques used to find vulnerabilities. MITRE, a not-for-profit based in Bedford, Mass., developed OVAL with help from industry, academia, and government organizations.

The language builds upon the *Common Vulnerabilities and Exposures* (www.cve.mitre.org), a dictionary of standard names and descriptions of existing information security openings. OVAL is a natural follow-on that will eliminate most ambiguity that currently plagues IT managers who are always on the lookout for the latest entry points for hackers.

"There are a number of tools that use *CVE*, but they all test for vulnerabilities in a different way," says Margie Zuk, program manager at MITRE. "You can use different tools running on the same systems and get different answers."

OVAL's introduction should change that. "Now people will have the tools to come to a consensus on the correct way to check for a given